



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/053,342	11/13/2001	Dinarte R. Morais	MS1-890US	6655

22801 7590 07/12/2005

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER

UNGAR, DANIEL M

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/053,342

Applicant(s)

MORAIS ET AL.

Examiner

Daniel M. Ungar

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on 13 November 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-54 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-54 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 13 November 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 7/22/04, 9/24/04.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

Art Unit: 2132

DETAILED OFFICE ACTION

1. Claims 1-54 have been examined.

CLAIM REJECTIONS - 35 U.S.C. 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -
(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 16, 18, 39, and 43-47 are rejected under 35 U.S.C. 102 as being anticipated by Chatani et al., U.S. Patent Application Publication Number 2002/0104019.

3. Regarding claims 16 and 18, Chatani et al. disclose retrieving a console-based key stored on a console, retrieving a title-based key associated with a game title running on the game console, and deriving one or more keys from the console-based and title-based keys (see paragraphs 0029, 0033-0036, 0051; figures 2B, 3A).
4. Regarding claim 39, Chatani et al. disclose obtaining a first and second key stored in memory associated with a game title running on a game console and deriving one or more keys from the first and second keys (see paragraphs 0029, 0033-0036, 0051; figures 2B, 3A).
5. Regarding claims 43-45, Chatani et al. disclose a memory to store a first key (see paragraphs 0016, 0024, 0032), a game title configured to execute on the game console, having an associated second key (see paragraph 0029), and a processor coupled to the memory, configured to derive at least one cryptographic key from the first and second key (see paragraphs 0016, 0032-0036; figures 2B, 3A).

Art Unit: 2132

6. Regarding claim 46, Chatani et al. disclose identifying a particular server hosting the game title among several servers, which meets the limitations of discovering another game console hosting the game title (see paragraph 0020).
7. Regarding claim 47, Chatani et al. disclose using the cryptographic key to establish a secure communication link with a remote game console over a network (see paragraphs 0003, 0019, 0032).

CLAIM REJECTIONS – 35 U.S.C. 103(a)

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 4-6, 8-13, 15, 19-26, and 48-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothschild et al., U.S. Patent Number 6,152,824, in view of Perlman, U.S. Patent Number 5,586,257.

9. Regarding claim 1, Rothschild et al. disclose a method comprising deriving a secret that is unique to a game console running a particular game title (see column 2, lines 1-14), and establishing a secure communications link between multiple game consoles over a network using the secret (see abstract; column 1, lines 27-43 and lines 59-67).

Although Rothschild et al. disclose various networks including the Internet and ISDN, they fail to explicitly disclose the network being a local area network. Nevertheless it was well known in the art at the time of the invention that multiple gaming consoles that communicate over a network such as the internet can communicate equally as well over a local area network. Exemplary of this is Perlman, who discloses a game operating over a LAN using the same

Art Unit: 2132

principles as a WAN (see column 34, line 66 – column 35, line 37). In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network, an equivalent network to the networks disclosed by Rothschild et al.

10. Regarding claim 4, Rothschild et al. disclose discovering whether another game console on the network is hosting the particular game title (see column 4, lines 4-18; column 7, lines 19-38), and exchanging secure communication keys between the multiple game consoles to facilitate secure multi-console play of the particular game title over the network (see column 4, line 52 – column 5, line 24; column 8, lines 35-62).

11. Regarding claim 5, Rothschild et al. does not disclose the network to comprise an Ethernet segment, but Ethernet was a well-known component of networks at the time of the invention. Exemplary of this is Perlman, who discloses Ethernet as part of the local area network. In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network using Ethernet.

12. Regarding claim 6, Rothschild et al disclose a method comprising:
generating at least one key that is secret to an authentic gaming system running an authentic game title (see column 4, lines 33-50; figure 7);
discovering whether another gaming system on a common network is hosting the game title (see column 4, lines 6-18); and
establishing a secure communication link between multiple gaming systems to facilitate multi-system play of the game title over the network (column 4, line 51 – column 5, line 24).

Although Rothschild et al. disclose various networks including the Internet and ISDN, they fail to explicitly disclose the network being a local area network. Nevertheless it was well known in

Art Unit: 2132

the art at the time of the invention that multiple gaming consoles that communicate over a network such as the internet can communicate equally as well over a local area network. Exemplary of this is Perlman, who discloses a game operating over a LAN using the same principles as a WAN (see column 34, line 66 – column 35, line 37). In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network, an equivalent network to the networks disclosed by Rothschild et al.

13. Regarding claim 8, Rothschild et al. disclose broadcasting a request to join in playing the game title being hosted by another gaming system (see column 4, lines 3-25; figure 8). Note that the server disclosed by Rothschild et al. is a gaming system that is a host, and meets the limitations as claimed.

14. Regarding claim 9, Rothschild et al. disclose a broadcast reply from the gaming system that is hosting the game title (see column 4, lines 19-25).

15. Regarding claim 10, Rothschild et al. disclose cryptographically encoding, using a generated key, a request to join in (see column 4, lines 3-25 and 52-59; column 5, lines 45-59); playing the game title being hosted by another gaming system (see column 6, lines 33-67; column 12, lines 1-13); and broadcasting the request over the network (see column 4, lines 3-25; column 7, lines 19-38; figure 8).

16. Regarding claim 11, Rothschild et al. does not disclose the network to comprise an Ethernet segment, but Ethernet was a well-known component of networks at the time of the invention. Exemplary of this is Perlman, who discloses Ethernet as part of the local area network. In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network using Ethernet.

Art Unit: 2132

17. Regarding claim 12, Rothschild et al. disclose exchanging secure communication keys between the multiple game consoles to facilitate multi-console play of the particular game title over the network (see column 8, lines 35-63).

18. Regarding claim 13, Rothschild et al. disclose broadcasting from a client game console over a network a request to join in playing a game title in a network gaming session being hosted by a host game console, the request containing a secret that is unique to the client game console running the game title, and broadcasting from the host game console over the network a reply to the request, the reply containing information that can be used to establish a secure communication link (see column 4, lines 4-59).

Although Rothschild et al. disclose various networks including the Internet and ISDN, they fail to explicitly disclose the network being a local area network. Nevertheless it was well known in the art at the time of the invention that multiple gaming consoles that communicate over a network such as the internet can communicate equally as well over a local area network. Exemplary of this is Perlman, who discloses a game operating over a LAN using the same principles as a WAN (see column 34, line 66 – column 35, line 37). In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network, an equivalent network to the networks disclosed by Rothschild et al.

19. Regarding claim 15, Rothschild et al. does not disclose the network to comprise an Ethernet segment, but Ethernet was a well-known component of networks at the time of the invention. Exemplary of this is Perlman, who discloses Ethernet as part of the local area network. In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network using Ethernet.

Art Unit: 2132

20. Regarding claims 19, 21, 22, 23, and 24, Rothschild et al. disclose creating a request to join in playing a game title being hosted by a host game console on the network and broadcasting the request over the network (see column 4, lines 4-18), receiving a reply from the host game console, the reply containing one or more session keys, and using the session keys from the reply to facilitate future secure communication with the host game console (see column 4, lines 19-25; column 4, line 52 – column 5, line 24).

Although Rothschild et al. disclose various networks including the Internet and ISDN, they fail to explicitly disclose the network being a local area network. Nevertheless it was well known in the art at the time of the invention that multiple gaming consoles that communicate over a network such as the internet can communicate equally as well over a local area network. Exemplary of this is Perlman, who discloses a game operating over a LAN using the same principles as a WAN (see column 34, line 66 – column 35, line 37). In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network, an equivalent network to the networks disclosed by Rothschild et al.

21. Regarding claim 20, Rothschild et al. does not disclose the network to comprise an Ethernet segment, but Ethernet was a well-known component of networks at the time of the invention. Exemplary of this is Perlman, who discloses Ethernet as part of the local area network. In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network using Ethernet.

22. Regarding claims 25 and 26, Rothschild et al. disclose in a networked gaming environment where multiple game consoles are connected via a network and at least two game consoles are playing a same game title, a method comprising:

forming an initial packet that contains first data used to derive a cryptographic key and computing a first hash digest of the initial packet (see column 5, lines 8-24);

sending the initial packet and the first hash digest to another game console on the network that is playing the same game title, and receiving a reply packet from the other game console, including a second hash digest and second data (see column 4, lines 4-18 and lines 52-59; column 6, lines 33-55); authenticating the reply packet using the second hash digest, and deriving one or more security association keys from the first and second data, the security association keys being used to secure communication between the multiple consoles (see column 4, lines 52 - column 5, line 24; column 8, lines 2-62).

Although Rothschild et al. disclose various networks including the Internet and ISDN, they fail to explicitly disclose the network being a local area network. Nevertheless it was well known in the art at the time of the invention that multiple gaming consoles that communicate over a network such as the internet can communicate equally as well over a local area network. Exemplary of this is Perlman, who discloses a game operating over a LAN using the same principles as a WAN (see column 34, line 66 - column 35, line 37). In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network, an equivalent network to the networks disclosed by Rothschild et al.

23. Regarding claim 48, Rothschild et al. disclose a memory and a processor coupled to the memory, configured to generate at least one key that is secret to the game console when running an authentic game title (see column 3, lines 37-49; column 4, line 33 - column 5, line 7), the processor being further configured to discover, using the key, a host game console on a network that is hosting the game title and to establish a secure communication link with the host game console over the local area network (see column 5, lines 45-59; column 6, lines 33-55).

Although Rothschild et al. disclose various networks including the Internet and ISDN, they fail to explicitly disclose the network being a local area network. Nevertheless it was well known in the art at the time of the invention that multiple gaming consoles that communicate over a network such as the internet can communicate equally as well over a local area network.

Art Unit: 2132

Exemplary of this is Perlman, who discloses a game operating over a LAN using the same principles as a WAN (see column 34, line 66 – column 35, line 37). In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network, an equivalent network to the networks disclosed by Rothschild et al.

24. Regarding claim 50, Rothschild et al. disclose discovering a host game console by creating a request to join in playing the game title and broadcasting the request over the network (see column 4, lines 4-25; column 5, lines 45-59).

25. Regarding claim 51, Rothschild et al. disclose establishing the secure communication link by exchanging data with the host game console that can be used to derive a cryptographic key (see column 5, lines 8-24)

68
26. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Chatani et al., as established above, ^{with respect to claim 16} in view of Murphy Jr. et al., U.S. Patent Number 6,006,266. Although Chatani et al. disclose deriving the key from the combination of the console-based key and the title-based key, they do not disclose the deriving as computing a hash function on a concatenation of the two keys. Nevertheless, hashing and concatenating two keys to derive a key was well known in the art at the time of the invention. Exemplary of this is Murphy Jr. et al. who disclose hashing and concatenating two keys to derive a single key comprised of the original two keys. In light of the teachings of Murphy Jr. et al. it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the keys using the method of Murphy Jr., in which the combination of the keys is more secure than two individual keys.

Art Unit: 2132

27. Claims 2, 3, 7, 14, 27, 30-38, 49, and 52-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothschild et al. in view of Perlman, as established above, further in view of Chatani et al., U.S. Patent Application Publication Number 2002/0104019.

28. Regarding claims 2 and 3, Rothschild et al. do not disclose keys for both the gaming system and the title, and deriving the key from the two. Nevertheless, creating a secret key by combining two keys was well known in the art at the time of the invention. Exemplary of this is Chatani et al., who in the similar field of endeavor of securing online games, disclose using both a console key and title key in combination (see paragraphs 0029, 0033-0036, 0051; figures 2B, 3A). In light of these teachings it would have been obvious to one of ordinary skill in the art to have required an additional key related to the game title in order to provide an extra layer of security.

29. Regarding claim 7, Rothschild et al. do not disclose keys for both the gaming system and the title, and deriving the key from the two. Nevertheless, creating a secret key by combining two keys was well known in the art at the time of the invention. Exemplary of this is Chatani et al., who in the similar field of endeavor of securing online games, disclose using both a console key and title key in combination (see paragraphs 0029, 0033-0036, 0051; figures 2B, 3A). In light of these teachings it would have been obvious to one of ordinary skill in the art to have required an additional key related to the game title in order to provide an extra layer of security.

30. Regarding claim 14, Rothschild et al. do not disclose keys for both the gaming system and the title, and deriving the key from the two. Nevertheless, creating a secret key by combining two keys was well known in the art at the time of the invention. Exemplary of this is Chatani et al., who in the similar field of endeavor of securing online games, disclose using both a console key and title key in combination (see paragraphs 0029, 0033-0036, 0051; figures 2B, 3A). In light of these teachings it would have been obvious to one of ordinary skill in the art to have required an additional key related to the game title in order to provide an extra layer of security.

Art Unit: 2132

31. Regarding claims 27 and 32, Rothschild et al. disclose:
- creating, at a first console, a request to join in playing the game title being hosted by a second game console on the network (see column 4, lines 4-18);
 - cryptographically encoding the request using the cryptographic key (see column 4, lines 33-50; column 6, lines 33-55);
 - broadcasting the request over the network (see column 5, lines 45-59);
 - cryptographically decoding the request, at the second game console, using the cryptographic key (see column 4, line 52 – column 5, line 7);
 - generating, at the second game console, a reply that contains at least one session key, cryptographically encoding the reply using the cryptographic key, and broadcasting the reply over the network (see column 5, lines 8-24 and lines 45-59);
 - cryptographically decoding the reply at the first game console, using the cryptographic key, and exchanging packets between the first and second game consoles, the packets being protected using the session key and containing data used to derive at least one security association key (see column 4, lines 19-25; column 6, lines 33-55); and
 - establishing a secure communication link between the first and second game consoles using the security association keys to facilitate secure multi-console play of the game title (see column 6, lines 33-55).

Rothschild et al. do not disclose keys for both the gaming system and the title, and deriving the key from the two. Nevertheless, creating a secret key by combining two keys was well known in the art at the time of the invention. Exemplary of this is Chatani et al., who in the similar field of endeavor of securing online games, disclose using both a console key and title key in combination (see paragraphs 0029, 0033-0036, 0051; figures 2B, 3A). In light of these teachings it would have been obvious to one of ordinary skill in the art to have required an additional key related to the game title in order to provide an extra layer of security.

Although Rothschild et al. disclose various networks including the Internet and ISDN, they fail to explicitly disclose the network being a local area network. Nevertheless it was well known in the art at the time of the invention that multiple gaming consoles that communicate over a network such as the internet can communicate equally as well over a local area network. Exemplary of this is Perlman, who discloses a game operating over a LAN using the same principles as a WAN (see column 34, line 66 - column 35, line 37). In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network, an equivalent network to the networks disclosed by Rothschild et al.

32. Regarding claim 30, Rothschild et al. disclose forming, at one of the first or second game consoles, a packet that contains the data used to derive the security association key (see column 4, line 51 - column 5, line 24; column 8, lines 2-62), computing a hash digest of the packet and sending the packet and the hash digest to the other of the first or second game consoles (see column 4, lines 4-18 and lines 52-59; column 6, lines 33-55), and authenticating the packet using the hash digest at the other first or second game consoles (see column 4, line 52 - column 5, line 24; column 8, lines 2-62).

33. Regarding claim 31, Rothschild et al. disclose the data used to derive the security association key comprises values used by a cryptographic Diffie-Hellman function (see column 4, line 52 - column 5, line 7).

34. Regarding claims 33-38, Rothschild et al. disclose
retrieving a console-based cryptographic key and creating a request to join in playing
the game title being hosted by another game console on the network, encoding
the request using the cryptographic key, broadcasting the request over the
network (see column 4, lines 4-50);
receiving a reply from a host game console, the reply containing at least one session key,
exchanging packets with the host game console, the packets being protected

using the session key and containing data used to derive at least one security association key, and establishing a secure communication link with the host game console using the security association key (see column 4, line 51 – column 5, line 24; column 34-55; column 8, lines 2-62).

Although Rothschild et al. disclose various networks including the Internet and ISDN, they fail to explicitly disclose the network being a local area network. Nevertheless it was well known in the art at the time of the invention that multiple gaming consoles that communicate over a network such as the internet can communicate equally as well over a local area network. Exemplary of this is Perlman, who discloses a game operating over a LAN using the same principles as a WAN (see column 34, line 66 – column 35, line 37). In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network, an equivalent network to the networks disclosed by Rothschild et al.

Rothschild et al. do not disclose keys for both the gaming system and the title, and deriving the key from the two. Nevertheless, creating a secret key by combining two keys was well known in the art at the time of the invention. Exemplary of this is Chatani et al., who in the similar field of endeavor of securing online games, disclose using both a console key and title key in combination (see paragraphs 0029, 0033-0036, 0051; figures 2B, 3A). In light of these teachings it would have been obvious to one of ordinary skill in the art to have required an additional key related to the game title in order to provide an extra layer of security.

35. Regarding claim 49, Rothschild et al. do not disclose second data associated with the game title and deriving the key from the two data. Nevertheless, creating a secret key by combining two keys was well known in the art at the time of the invention. Exemplary of this is Chatani et al., who in the similar field of endeavor of securing online games, disclose using both a console key and title key in combination (see paragraphs 0029, 0033-0036, 0051; figures 2B, 3A). In light of these teachings it would have been obvious to one of ordinary skill in the art to

Art Unit: 2132

have required additional data related to the game title in order to provide an extra layer of security.

36. Regarding claims 52 and 53, Rothschild et al. disclose first and second game consoles with network connections to facilitate connection to a network, the first and second consoles running the same game title, and the first game console being configured to discover the second game console by broadcasting messages over the network, the messages being secured by keys (see column 4, lines 4-25 and lines 52-59; column 5, lines 45-59).

Although Rothschild et al. disclose various networks including the Internet and ISDN, they fail to explicitly disclose the network being a local area network. Nevertheless it was well known in the art at the time of the invention that multiple gaming consoles that communicate over a network such as the internet can communicate equally as well over a local area network. Exemplary of this is Perlman, who discloses a game operating over a LAN using the same principles as a WAN (see column 34, line 66 – column 35, line 37). In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network, an equivalent network to the networks disclosed by Rothschild et al.

Rothschild et al. do not disclose the two consoles generating identical keys by virtue of the same game title. Nevertheless, generating a unique key for a particular title, common to consoles running the same title, was well known in the art at the time of the invention. Exemplary of this is Chatani et al., who in the similar field of endeavor of securing online games, discloses a title key that is generated by consoles running that title (see paragraphs 0029, 0033, 0036; figures 2B, 3A). In light of these teachings it would have been obvious to one of ordinary skill in the art to have utilized the title in creating the key shared between the two consoles in order to authenticate the title as well as the console.

Art Unit: 2132

37. Regarding claim 54, Rothschild et al. does not disclose the network to comprise an Ethernet segment, but Ethernet was a well-known component of networks at the time of the invention. Exemplary of this is Perlman, who discloses Ethernet as part of the local area network. In light of the teachings of Perlman it would have been obvious to one of ordinary skill in the art at the time of the invention to have communicated over a local area network using Ethernet.

38. Claims 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothschild et al. in view of Perlman, as established above, further in view of Nguyen, U.S. Patent Application Publication Number 2002/0071557.

39. Regarding claim 40, Rothschild et al. disclose computer-readable medium for a game console comprising computer-executable instructions that, when executed, direct the game console to:

encrypt a request to join in playing a game title being hosted by a remote host game console on a network (see column 4, lines 4-25 and lines 52-59);

broadcast the request over the network and listen for at least one broadcast reply from the host game console (see column 4, lines 19-25);

upon receipt of the reply, extract at least one session key from the reply for use in facilitating future communication with the host game console (see column 5, lines 8-24);

form an initial packet that contains first data used to derive a cryptographic key and compute a first hash digest of the initial packet using the session key (see column 4, line 51 – column 5, line 24; column 8, lines 2-62);

send the initial packet and the first hash digest to the host game console, listen for a reply packet from the host game console, the reply packet including a second hash digest and second data, and authenticate the reply packet using the session

Art Unit: 2132

key and the second hash digest (see column 4, lines 4-18 and lines 52-59; column 6, lines 33-55); and

derive at least one security association key from the first and second data, the security association keys being used to secure communication with the host game console (see column 4, line 52 - column 5, line 24; column 8, lines 2-62).

Rothschild et al. do not disclose digitally signing the reply. Nevertheless, Nguyen, in the similar field of endeavor of secure network gaming, discloses communication between two gaming machines wherein the reply includes a digital signature (see column 0017, 0056, 0059, Claim 47). It would have been obvious to one of ordinary skill in the art at the time of the invention to have included digital signatures in the authentication method of Rothschild et al. in order to ensure that the reply came from the authentic sender, an objective of authentication.

40. Regarding claims 41 and 42, Rothschild et al. disclose a computer-readable medium for a game console comprising computer-executable instructions that, when executed, direct the game console to:

receive a request from a remote game console on a network, the request seeking network play of a game title (see column 4, lines 3-18);

authenticate the request as being generated by an authentic game console running an authentic version of the game title, decode the request, and determine whether to allow the remote game console to play (see column 6, lines 33-67; column 8, lines 2-62);

in an event the remote game console is allowed to play, create a reply with containing at least one session key, and send the reply to the remote game console (see column 5, lines 8-24);

receive an initial packet directly from the remote game console, the initial packet containing first data used to derive a cryptographic key, authenticate the initial

packet using the session key and form a response packet holding second data used to derive a cryptographic key (see column 6, lines 33-55);
send the response packet to the remote game console and derive at least one security association key from the first and second data, the security association keys being used to secure communication with the remote game console (see column 8, lines 2-62).

Rothschild et al. do not disclose digitally signing the reply. Nevertheless, Nguyen, in the similar field of endeavor of secure network gaming, discloses communication between two gaming machines wherein the reply includes a digital signature (see column 0017, 0056, 0059, Claim 47). It would have been obvious to one of ordinary skill in the art at the time of the invention to have included digital signatures in the authentication method of Rothschild et al. in order to ensure that the reply came from the authentic sender, an objective of authentication

41. Claim 28 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rothschild et al. in view of Perlman and Chatani et al., as established above, further in view of Murphy Jr. et al., U.S. Patent Number 6,006,266. Although Chatani et al. disclose deriving the key from the combination of the console-based key and the title-based key, they do not disclose the deriving as computing a hash function on a concatenation of the two keys. Nevertheless, hashing and concatenating two keys to derive a key was well known in the art at the time of the invention. Exemplary of this is Murphy Jr. et al. who disclose hashing and concatenating two keys to derive a single key comprised of the original two keys. In light of the teachings of Murphy Jr. et al. it would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the keys using the method of Murphy Jr. The motivation of combining keys to begin with is taught by Chatani et. al.

42. Claim 29 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rothschild et al. in view of Perlman and Chatani et al., as established above, further in view of Nguyen, U.S.

Art Unit: 2132

Patent Application Publication Number 2002/0071557. Rothschild et al. do not disclose digitally signing the reply or computing an encryption key. Nevertheless, Nguyen, in the similar field of endeavor of secure network gaming, discloses communication between two gaming machines wherein the reply includes a digital signature (see column 0017, 0056, 0059, Claim 47). It would have been obvious to one of ordinary skill in the art at the time of the invention to have included digital signatures in the authentication method of Rothschild et al. in order to ensure that the reply came from the authentic sender, an objective of authentication.

CONCLUSION

43. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel M. Ungar whose telephone number is 571.272.7960. The examiner can normally be reached on 8:30 - 6:00 Monday - Thursday, Alt. Fridays.

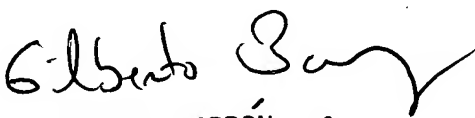
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571.272.3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Art Unit 2132



Daniel Ungar



GILBERTO BARRÓN JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100